IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** v. **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

DECLARATION OF J. ALEX HALDERMAN IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION

J. ALEX HALDERMAN declares, under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

Georgia's Election System Improvements Are Insufficient

2. State Defendants highlight a number of purported improvements to Georgia's election security that have been implemented since September 2018. Some of these long overdue changes are steps in the right direction. Others are mere window dressing. But these improvements do not add up to a remedy for the wide array of vulnerabilities posed by Georgia's election system.

3. As an initial matter, developments since September 2018 demonstrate that Curling Plaintiffs' concerns about Georgia's election system were justified, if not understated:

4. Georgia's online voter registration was shown to have serious, remotely exploitable vulnerabilities on the eve of a major election.[1]

5. The National Academies of Science, Engineering, and Medicine ("NASEM") concluded that there is scientific consensus that "[e]lections should be conducted with human-readable paper ballots", and that paperless DREs "should be removed from service as soon as possible."[2]

6. The Mueller Report outlined the scale and sophistication of Russia's efforts to interfere in the 2016 election, leaving no doubt that Russia and other adversaries will strike again.[3]

7. Despite these indications that Georgia's election security was and is vulnerable, the State has not even taken the rudimentary step of updating the software on its voting machines. Indeed, despite the fact that severe, remotely exploitable vulnerabilities exist in the State's voting machine firmware—and have

[1] Matt Bernhard. *Serious Vulnerabilities in Georgia's Online Voter Registration System*, (Nov. 4, 2018) https://medium.com/@mattbernhard/serious-vulnerabilities-in-georgias-online-voter-registration-system-cc319cbbe3d8.

[2] *New Report Identifies Steps to Secure Americans' Votes*, NASEM, (Sept. 6, 2018), https://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=25120

[3] Robert Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, (April 18, 2019) https://www.justice.gov/storage/report.pdf

been publicly known since 2007[4]—the State has not upgraded that firmware *since 2005*. Some—but not all—of these known vulnerabilities could be addressed merely by installing the latest software.

8. While Georgia has committed to implementing a new election system, the pace of its implementation is simply too slow. Until a reliable paper trail and statistically rigorous audits are implemented, Georgia's election system will remain vulnerable. The pace of its implementation makes clear that Georgia has not internalized the seriousness of the threats facing its election system.

9. While Georgia touts its reliance on DHS monitoring and scanning,[5] DHS has never conducted a forensic review of Georgia's—or any state's—DRE machines.[6] And, while DHS specifically called on election officials in all fifty states to implement verifiable ballots, Georgia still has not done so.[7]

10. Georgia notes that it has established endpoint protection on all computer servers and desktops in the CES that are *not* in the air-gap environment.[8]

[4] J. A. Calandrino, A. J. Feldman, J. A. Halderman, D. A. Wagner, H. Yu, and W. Zeller. *Source Code Review of the Diebold Voting System*, in Cal. Sec'y of State, *Top-to-Bottom Review* (2007), http://www.sos.ca.gov/elections/votingsystems/oversight/top-bottom-review/.

[5] (Decl. S. Merritt Beaver ("Beaver Decl."), ¶¶ 5, 10, ECF No. 472-2.)

[6] Mark Sullivan, *Two and a half years later, DHS still hasn't performed audits to see if votes were hacked in 2016*, Fast Company, (May 16, 2019), https://www.fastcompany.com/90341582/two-and-a-half-years-later-dhs-still-hasnt-performed-audits-to-see-if-votes-were-hacked-in-2016

[7] Olivia Beavers, *DHS chief calls on officials in all 50 states to have 'verifiable' ballots by 2020 election*, The Hill, (Aug. 22, 2018), https://thehill.com/policy/cybersecurity/403148-dhs-chief-calls-on-election-officials-in-all-50-states-to-have

[8] (Beaver Decl. ¶ 7.)

This is baffling. The computer servers and desktops within the air-gap environment are presumably the most sensitive servers and desktops within CES. These computers and servers need *at least* as strong a defense.

11. Georgia notes that it has moved all ballot building and ExpressPoll dataset production to the office of the Georgia Secretary of State (the "SOS").[9] But, like Kennesaw State before it, the SOS office has a poor record of securing critical election systems, including the online voter registration system discussed above. Furthermore, regardless of where these activities physically take place, these critical processes still rely on the same vulnerable GEMs software as they did at Kennesaw State.

12. Georgia touts its new GEMS database transmittal procedures.[10] These procedures largely amount to password-protecting and encrypting the CDs used to transfer GEMS data to counties. Although this protection might help safeguard the data from disclosure, it does not appear to adequately protect the data from malicious modification while the CDs are in transit. This procedure also potentially creates a further route by which malware could spread to county GEMS servers: an attacker could infect the CD with malware that would spread to the county GEMS server when county officials extract the database. In any event, these procedures do not

[9] (Beaver Decl. ¶ 5.)
[10] (Beaver Decl. ¶ 14.)

address the potential for an attacker to modify the GEMS database before it is password-protected and encrypted, and none of the State's new procedures would detect such a modification.

13. Georgia notes that "Albert sensors" are now in place at the point that the Secret of State's network connects to the Internet.[11] Albert sensors scan network traffic for known patterns associated with specific attacks. Albert sensors are limited in that they only can detect known, specific attack signatures, they can only monitor network traffic passing specific locations, and they can only analyze specific forms of network traffic. Albert sensors also do not monitor malware or other attacks introduced through physical access to servers or other systems.

14. Notably, some of the "improvements" that Georgia emphasizes are outdated. For example, Georgia now requires SOS employees to establish "complex sixteen (16) character passwords."[12] But the Department of Commerce's National Institute of Standards and Technology ("NIST") recommends that users not rely on "convoluted and complex passwords that make no sense to the user."[13] Instead,

[11] (Beaver Decl. ¶ 23.)

[12] (Beaver Decl. ¶ 23.)

[13] Craig Pollack, *Surprising Password Guidelines from NIST You Should Know*, (Oct. 16, 2018), FPA Technology Services https://www.fpainc.com/blog/password-guidelines-from-nist (citing Paul A. Grassi, Michael E. Garci, James L. Fenton, *Digital Identify Guidelines*, NIST, (June 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

current guidelines are "focused on creating unique passphrases that users will remember easily, using whatever characters they want."[14]

15. Georgia's improvements largely are procedural controls—that is, controls resting entirely on the ability of SOS employees to correctly complete certain steps and make certain checks. But SOS employees have a long history of procedural missteps. For example, in 2015, while Mr. Beaver was in his current role as Chief Information Officer, the SOS's office accidentally (and illegally) mailed 6.2 million Georgia voters' social security numbers and other information to State political parties, news media organizations, and Georgia GunOwner Magazine.[15] SOS Kemp blamed this squarely on an employee: "This employee violated six different internal policies resulting in the release of data."[16] Notably absent from Mr. Beaver's declaration is a description of the training protocols that have been put in place to ensure that SOS employees actually follow any new procedural controls.

16. Indeed, SOS employees' attentiveness to cybersecurity remains lax. CES Director Barnes testified at his deposition that he relies upon a USB drive to transfer GEMS export files between GEMS and his laptop.[17] Such a USB stick, if

[14] *Id.*

[15] Kristina Torres, *Data breach in Georgia could affect 6 million voters*, The Atlanta Journal-Constitution, (Nov. 18, 2015), https://www.ajc.com/news/state--regional-govt--politics/data-breach-georgia-could-affect-million-voters/QyTFJeWuvAFVg2K7HGYvuN/.

[16] Kristina Torres, *Exclusive: Fired Kemp worker says he's a scapegoat in data breach*, The Atlanta Journal-Constitution, (Dec. 2, 2015), https://www.ajc.com/news/state--regional-govt--politics/exclusive-fired-kemp-worker-says-scapegoat-data-breach/m1yBjy5dQVqNs4hAiQay1J/.

[17] (Barnes Dep. at 228:22-230:5.)

infected with malware, could subvert the entire Georgia election system. Barnes attempts to keep the USB drive secure by keeping it in a locked drawer in his desk.[18] Barnes admitted, however, that the key to this drawer was left in a different unlocked drawer in the same desk.[19]

17. Further, none of Georgia's purported improvements address any of the vulnerabilities of GEMS servers operated by counties.

[redacted]

[18] (*Id.* at 233:19-234:1.)
[19] (*Id.* at 234:2-17.)
[redacted]

[redacted]

[redacted]

[redacted]

Dr. Shamos is an Outlier

24. In the course of my work involving election cybersecurity, I have occasionally come across Dr. Shamos' statements regarding election security. Based upon my review of his public statements, as well as his background, I consider Dr. Shamos an uninformed outlier.

25. Dr. Shamos has no relevant expertise in computer security. He has never published a peer-reviewed technical paper regarding election security. His uninformed opinions run contrary to the last decade of research and development in the field of election security, findings by the U.S. Senate Select Committee on Intelligence, and the consensus view of the National Academies of Science, Engineering, and Medicine.

26. While he served as a statutory voting examiner, his role required no qualifications or experience in computer security. This was unfortunate, because his work as a statutory voting examiner clearly would have benefited from having such qualifications or experience. Dr. Shamos repeatedly failed to detect problems in voting systems that were later discovered by security experts to have significant security vulnerabilities.

[redacted]

27. Throughout his career, Dr. Shamos has repeatedly made bold proclamations such as those made here: "there has never been a verified incident of tampering with an electronic voting machine in an election;"[32] "despite the existence of so many vulnerabilities, no one has exploited them in an election;"[33] Russia did not attack Georgia's voting system[34]; Russia has no ability to attack Georgia's system except through the Internet.[35] Consistent with Dr. Shamos' past unsupported claims, he provides absolutely no basis for these contentions. Dr. Shamos does not state that he has inspected any of the machines at issue or any other aspect of Georgia's election systems. Nor does he claim to be in possession of non-public information concerning Russian cyberattack capabilities or targets. The only way one could conclusively determine that Georgia's election systems had not been hacked is with an auditable, voter-verifiable system. Georgia does not have such a system, because it relies on vulnerable and outdated DRE technology.

28. Dr. Shamos repeatedly attacks the use of paper ballots.[36] This, notwithstanding the fact that he has never published a scientific study regarding the security of paper ballot voting systems. Notably, he does not square his criticisms of paper ballots with the fact that Georgia uses such ballots for absentee and

[32] (Decl. Michael Shamos, PH.D., J.D. ("Shamos Decl.") ¶ 33 ECF No. 472-1.)
[33] (*Id.* ¶ 138.)
[34] (*Id.* ¶ 139.)
[35] (*Id.* ¶ 64.)
[36] (*See id.* ¶¶ 35-50.)

provisional voting, or that Georgia intends to adopt a paper ballot system. Nor does he address the fact that both the U.S. Senate Select Committee on Intelligence and the National Academies have emphasized the urgent need for all states to implement paper ballot voting systems.[37]

29. Paper ballots can, of course, be tampered with. Notably, however, almost all of the instances of reported fraud and election-related convictions that Dr. Shamos cites involve absentee ballots or voter-registration fraud, and not in-precinct paper ballots or ballot counting.[38] Because these types of attacks are relatively unsophisticated compared to the types of attacks potentially facing DRE voting systems, they are naturally easier to detect. By comparison, the threats facing DREs—including attacks from foreign nations—are sophisticated and difficult to detect.

30. While paper ballots do, of course, need to be secured with careful chain-of-custody procedures to provide protection against physical manipulation, the physical security required for handling paper ballots is actually less than the physical security required in a DRE system. In a DRE system, machines and their data need

[37] *See Senate Intel Committee Releases Unclassified 1st Installment in Russia Report, Updated Recommendations on Election Security*, Senate Select Committee on Intelligence, (May 8, 2018), https://www.warner.senate.gov/public/index.cfm/2018/5/senate-intel-committee-releases-unclassified-1st-installment-in-russia-report-updated-recommendations-on-election-security; *New Report Identifies Steps to Secure Americans' Votes*, NASEM, (Sept. 6, 2018), https://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=25120

[38] (Shamos Decl. ¶¶ 31, 39.)

to be safeguarded against physical handling at *all times*, from the moment the machines and software are manufactured to the last time they are used in election. The physical media needs to be safeguarded, and so do the servers used to program ballots and tabulate results. Any lapse can result in the machines being permanently untrustworthy. In contrast, paper ballots need only be safeguarded between voting and counting (including any post-election audits or recounts).

31. Many of Dr. Shamos's strongest criticisms of paper ballots simply do not apply to the kind of paper ballot system that Plaintiffs are seeking. They are seeking what is called precinct-count optical scan voting ("PCOS"), a modern voting method that is widely used across the country. PCOS involves voters marking a paper ballot in a precinct and feeding it into an optical scanner attached to a ballot box. The scanner is a computer that recognizes marks on the paper and records the ballot contents to a removable memory card. The machine can recognize undervoted or overvoted ballots and return them to the voter for correction.

32. PCOS systems, coupled with effective chain of custody procedures and rigorous auditing of the paper ballots, offer excellent security. PCOS scanners create dual records of every ballot, one on paper and one in electronic form, both created at the moment the ballot is cast. Having dual records is safer than having only a paper record or only an electronic record, since, as long as the records are rigorously audited to ensure that they agree about the outcome, an attacker would have to cheat

on both sets of records in order to avoid the fraud being detected. This makes PCOS less risky than other forms of paper balloting (such as hand counting and vote-by-mail) and far less risky than paperless DRE voting.

33. PCOS scanners, like DREs, are potentially vulnerable to hacking that alters the electronic results.[39] By auditing the paper record, however, we can detect and correct any outcome-changing fraud. I have published multiple peer-reviewed studies about methods for using paper to detect and correct attacks against optical scanners[40,41].

34. Apparently ignoring Dr. Shamos' advice, Georgia has already committed to implementing a PCOS voting system and audits. The only question remaining is how quickly and effectively Georgia will implement such a system.

35. Dr. Shamos also voices the concern that optical scanners may retain ballots in the order in which they were cast, thus compromising voters' privacy.[42] I share this concern, which may apply to many optical scan systems. Well-designed PCOS scanners, however, ensure that ballots are shuffled as they are accumulated

[39] I myself have discovered such vulnerabilities in the California Top-to-Bottom Review. *See* California Secretary of State's Office. "Top-to-Bottom" Review of voting systems, main website, 2007. http://www.sos.ca.gov/elections/ voting-systems/oversight/top-bottom-review/.

[40] J. A. Calandrino, J. A. Halderman, and E. W. Felten, "Machine-Assisted Election Auditing." In *USENIX/ACCURATE Electronic Voting Technology Workshop* (2007).

[41] Kellie Ottoboni, Matthew Bernhard, J. Alex Halderman, Ronald L. Rivest, and Philip B Stark. "Bernoulli Ballot-Polling: A Manifest Improvement for Risk-Limiting Audits." In *4th Workshop on Advances in Secure Electronic Voting* (2019).

[42] (Shamos Decl. ¶ 59.)

inside the ballot box. I strongly recommend that Georgia select equipment capable of this. Notably, Georgia's current DREs also store electronic records of votes in the order in which they are cast. Dr. Shamos and I appear to agree that Georgia's current system compromises privacy.

36. Dr. Shamos correctly notes that in some cases a voter may fail to follow directions when marking paper ballots.[43] These usability issues can be minimized by following recommended ballot design practices published by the American Institute of Graphic Arts in conjunction with the U.S. Election Assistance Commission.[44]

37. Dr. Shamos does not appear familiar with modern optical scanning equipment. Indeed, modern optical scanners are far more capable of recognizing imperfect marks than the older generations of equipment he describes. They are nothing like "hanging chad" style punch-card ballots, which were the subject of attention almost two decades ago.[45]

38. Dr. Shamos appears badly uninformed with respect to the basic computer security attributes of Georgia's DRE system. He claims that a large-scale cyberattack would require "unlimited access to each machine of a population of tens

[43] (Shamos Decl. ¶¶ 48-49.)

[44] *See Ballot and polling place design guidelines*, American Institute of Graphic Arts, https://www.aiga.org/aiga/content/why-design/design-for-democracy/ballot-and-polling-place-design-guidelines/.

[45] (*See* Shamos Decl. ¶ 47.)

of thousands."[46] Not so. An attack that successfully infiltrated the State's GEMS servers could spread to the entire state. Similarly, an attack that successfully infiltrates a county GEMS server could spread to the entire county. Neither attack would require discovering new vulnerabilities, but merely exploiting the vulnerabilities documented by the California and Ohio Secretaries of State in 2007.

39. The same is true with respect to Dr. Shamos' contention that attacks would require physical access to voting machines[47] and that "no one has shown an attack that would 'cause the machines to fail to operate on election day.'"[48] I personally have demonstrated in peer-reviewed research that attacks would not necessitate physical access to voting machines and that an attack could cause voting machines to fail to operate on election day.[49]

40. Similarly, Dr. Shamos claims that "[n]o one has shown that the AccuVote software that reads memory cards is susceptible to buffer overflows."[50] Again, I myself have shown such vulnerabilities in 2007, as part of the California Top-to-Bottom Review. These are one of the most serious kinds of vulnerabilities that could affect a DRE, and it is shocking that Dr. Shamos is unaware of them. This

[46] (Shamos Decl. ¶ 70.)
[47] (Shamos Decl. ¶ 72.)
[48] (Shamos Decl. ¶ 69.)
[49] Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, "Security Analysis of the Diebold AccuVote-TS Voting Machine." In *2007 USENIX/ACCURATE Electronic Voting Technology Workshop* (2007).

misunderstanding apparently forms the basis for his opinion that a "Stux-net" style attack would not succeed in Georgia.[51]

41. Dr. Shamos also mistakenly asserts that a vote-shifting algorithm would create obviously wrong results and thus be detected.[52] There are many different algorithms an attacker could use to determine how many votes to shift, from where to shift those votes, and in favor of which candidate. As a very simple example, an attacker could shift a fraction of the vote (e.g., 5% of votes for candidate A are switched to votes for candidate B). Such a shift would not necessarily be detectable, particularly in elections with limited or unreliable polling data.

42. Dr. Shamos defends the use of tamper-evident seals, claiming that circumventing such seals would cost an attacker precious time. He seems unaware of work by Appel,[53] Johnston,[54] and other authors that shows how seals can be removed and replaced quickly without detection.

43. Dr. Shamos mistakenly claims that malware could be detected by comparing the software on an administrative computer to the manufacturer's hash

[52] (*Id.* ¶ 76.)
[53] *See* Andrew W. Appel, *Security Seals on Voting Machines: A Case Study*, (2011), https://www.cs.princeton.edu/~appel/voting/SealsOnVotingMachines.pdf.
[54] Roger G. Johnson, *Tamper-Indicating Seals*, American Scientist (Nov. 2006), https://www.researchgate.net/publication/270405619_Tamper-Indicating_Seals.

for such software stored at NIST.[55] Malware would not have to change any of the files for which a manufacturer's hash was recorded by NIST.

44. Not content to be mistaken just as to election software, Dr. Shamos extends his lack of understanding to automobile software, mistakenly asserting that the Volkswagen emission software had a "test mode."[56] Volkswagen's emission software did not have a test mode.[57] Instead, Volkswagen's emission-cheating software was designed to detect the scripted conditions of an emissions test and disable itself while a vehicle was being tested. In exactly this manner, an attacker could manipulate Dr. Shamos's parallel testing to evade detection.

45. Dr. Shamos suggests a number of potential means of mitigating the attacks described in my testimony and declarations.[58] Most of these mitigations would be impractical, ineffective, or both. Moreover, even if these defenses worked in theory, Georgia *does not and has never employed them*. Therefore, the risks posed by these attacks remain.

46. For example, Dr. Shamos proposes verifying the integrity of individual memory cards at each precinct. As he explains, "[t]he individual precincts, prior to installing the memory card, would plug it into a PC to compute its hash value, which

[55] (Shamos Decl. ¶ 133.)

[56] (Shamos Decl. ¶ 134.)

[57] *See* Mortiz Contag, Guo Li, Andre Pawlowski, Felix Domke, Kirill Levchenko, Thorsten Holz, and Stefan Savage, *How They Did It: An Analysis of Emission Defeat Devices in Modern Automobiles*, http://cseweb.ucsd.edu/~klevchen/diesel-sp17.pdf

[58] (Shamos Decl. ¶¶ 77, 98, 99, 101, 103, 132.)

would then be compared with the true value."[59] But Dr. Shamos's proposed solution would create an additional way that memory cards could be infected by malware: directly from a PC used within each individual precinct for verification. Further, Dr. Shamos procedure presumes that there would be some uninfected copy of the memory with which to compare. An attack that infected the state or county GEMS system could infect *every* copy of the memory card. In any event, Georgia does not verifying the integrity of individual memory cards at each precinct.

47. Dr. Shamos also proposes performing forensic investigations of machines before or during elections.[60] Notably, Georgia conducts no such forensic investigation of its DRE machines.

48. Dr. Shamos further proposes parallel testing of DRE machines.[61] Notably, however, the "parallel testing" described by Dr. Shamos does not match how Georgia actually conducts the process. According to Dr. Shamos, "proper" parallel testing involves: (1) selecting a precinct at random and designating a machine to be voted on; (2) generating ballots at random based on the political demographics of the precinct; (3) conducting parallel testing while the election is in progress; and (4) asking poll workers to observe real voters from a distance and vote

[59] (*Id.* ¶ 77.)
[60] (Shamos Decl. ¶ 103.)
[61] (Shamos Decl. ¶¶ 97-101.)

at the same pace as they do.[62] In Georgia, however, a GEMS database is set up by at an SOS facility.[63] Ballots are not generated at random based on the political demographics of a given precinct.[64] No actual voters are observed, and thus ballots are not entered at the same pace as actual voters.[65] To the contrary, ballots are artificially entered every hour.[66] Dr. Shamos implies that each of these lapses creates opportunities for malware to circumvent parallel testing.

49. More alarming, however, is that Georgia only conducts parallel testing on a single machine. If only a fraction of Georgia's DRE machines were to be infected, or if all machines were infected with malware that only cheated a fraction of the times the machine was turned on, parallel testing of a single machine would, at best, detect malware with that fraction probability. For example, if an attacker infected 20% of Georgia's DRE machines, they would have at least an 80% chance of escaping detection during parallel testing.

[62] (Shamos Decl. ¶¶ 98- 99

[63] (Beaver Decl. ¶ 18.)

[64] (*Id.*)

[65] (*Id.*)

[66] (*Id.*)

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 18th day of July, 2019 in Cambridge, Massachusetts.

J. ALEX HALDERMAN